IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Siegried KOEPPEN et al.

Conf. No.: 8841

Application No.: 10/563,337

Art Unit: 2431

Filed: January 3, 2006

Examiner: Sarah Su

For: METHOD FOR USE IN A NETWORK BASED SAFETY DATA STORAGE SYSTEM

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

MS Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

September 11, 2009

Dear Sir:

Appellants submit this Brief in accordance with 37 C.F.R. § 41.37 in support of their appeal from the Final Office Action, February 18, 2009 by Examiner Sarah Su, the Advisory Action, mailed May 6, 2009, and the Notice of Panel Decision from Pre-Appeal Brief, mailed August 12, 2009, in the above-identified patent application.

In accordance with 37 C.F.R. §§ 41.31 and 41.37, this brief follows the June 18, 2009 filing of a Notice of Appeal and payment of the required fee. The filing of this Appeal Brief requires no extension of time fee. However, the Commissioner is hereby authorized to charge any unpaid fees deemed required in connection with this Appeal Brief, or to credit any overpayment, to Deposit Account No. 04-0100.

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Deutsche Telekom AG. The inventors having assigned their rights in and to this application to Deutsche Telekom AG, such assignment having been duly recorded.

II. RELATED APPEALS AND INTERFERENCES

To appellants' knowledge, there are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 2-16 are pending in the application.

This appeal is in respect of the rejection of claims 2-16.

There are 15 claims pending in the application, *i.e.*, claims 2-16. They are reproduced in the **Claims Appendix**. The current status of the application's claims is as follows:

1. Claims canceled: 1;
2. Claims withdrawn from consideration but not canceled: none;
3. Claims pending: 2-16;
4. Claims allowed: none;
5. Claims rejected: 2-16.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the mailing of the May 6, 2009 Advisory Action, which entered the claim amendments submitted April 17, 2009 in an Amendment After Final Office

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed invention provides a method for data storage on a server in a telecommunications network. A method for data storage on a server in a telecommunications network includes issuing (on request by an operator of a server) to a first user of the users a user certificate for access conditions, providing the user certificate and a secret key to the first user, accessing the server over an internet, sending (by the server) a client program to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement, setting up a personal main folder on the server for the first user, the main folder having a first special file including a first security requirement defined for the main folder and first management information so as to provide a main locker, configuring the personal main folder to have at least one further folder set up therein, the at least one further folder having a function and a second file including a second security requirement defined for the least one further folder and including second management information so as to provide a functional locker, displaying the functional locker only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, wherein the functional locker provides a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user, and at

least one of: a provisioning locker, wherein a first reference to a different second file available to another user is storable therein only by the first user, and a receiving locker, wherein a third file of a second user of the users is storable therein only by the second user, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement. (Specification, ¶¶ 0012, 14-16, 18-21, 29-30 and 32; Table 1.)

Independent method claim 2 is directed to a "method for data storage on a server in a telecommunications network" where the telecommunications network provides connectivity between local computers of users and the server, and recites the steps of "issuing, upon request, by an operator of the server, to a first user of the users a user certificate for access conditions" (Specification, ¶ 0012; Fig. 2, item 8, 10), "providing the user certificate and a secret key to the first user" (Specification, ¶ 0012; Fig. 2, item 8, 10), "accessing the server over an internet" (Specification, ¶ 0019; Fig. 1), "sending, by the server, a client program to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement" (Specification, ¶¶ 0015, 20 and 21; Fig. 2), "setting up a personal main folder on the server for the first user, the main folder having a first special file including a first security requirement defined for the main folder and first management information so as to provide a main locker" (Specification, ¶¶ 0014-15, Table 1; Fig. 3, item 1), "configuring the personal main folder to have at least one further folder set up therein, the at least one further folder having a function and a second file including a second security requirement defined for the least one further folder and including second management information

so as to provide a functional locker" (Specification, ¶¶ 0015-16; Fig. 3, item 2-5), "displaying the functional locker only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, wherein the functional locker provides a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user" (Specification, ¶¶ 0015-16 and 18; Fig. 3, item 2, 7), and at least one of: "a provisioning locker, wherein a first reference to a different second file available to another user is storable therein only by the first user" (Specification, ¶¶ 0016, 18, 29 and 32; Fig. 3, item 3, 7), and "a receiving locker, wherein a third file of a second user of the users is storable therein only by the second user, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement" (Specification, ¶¶ 0016, 18, 30 and 32; Fig. 3, item 4, 7).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) Whether claims 2-16 can properly be rejected as obvious under 35 U.S.C. § 103(a) based on respective combinations of U.S. Published Application No. 2004/0054750 to de Jong et al. ("de Jong"), U.S. Published Application No. 2003/0174842 to Challener, U.S. Patent No. 5,901,227 to Perlman, and U.S. Published Application No. 2004/0010715 to Winiger et al. ("Winiger").

VII. ARGUMENT

Grounds of Rejection No. 1: Obvious rejection of claims 2-16 based on respective combinations of de Jong, Challener, Perlman, and Winiger

De Jong describes a system for digital access control in which a content rights database 2714 stores an association between a user 2702 and a description of digital content that the user is

authorized to access. A content producer 2710 provides digital content to a content repository 2708, and provides a description of the content to a content provisioner 2724. De Jong, ¶¶ 0169-170; Fig. 27. De Jong describes that a particular content producer 105-120 controls access to digital content stored by the digital content producer. De Jong further describes that a user desiring access to digital content stored by a content producer 105-120 uses a mobile phone 125-140 to issue an access request to the particular content producer. De Jong, ¶¶ 007-08; Fig. 1. De Jong describes that a download manager 2716 is configured to receive a digital content request and communicate with a content rights database 2722 to determine whether the user is authorized to access the digital content provided by the content producer 2710. A content repository 2708 is configured to receive an authenticated digital content request and return digital content corresponding to the authenticated digital content request. The content producer 2710 provides digital content to the content repository 2708. De Jong, ¶¶ 0170-175; Fig. 27.

Thus, there is a clear distinction in de Jong between the user 2702 (*i.e.*, one who issues an access request) and the content producer 2710 (i.e., a system component that stores digital content or a reference to the digital content). Nowhere does de Jong teach or suggest that a user stores content or a reference to the content, as required by the present claims (see below).

Challener describes a system and method for storing a user's private key on a TCPA-enabled server. Abstract. Challener describes that asymmetric encryption is performed using both a public key and a private key. The private key is only available to a recipient of a confidential communication. Challener, ¶ 0004.

Independent claim 2 of the present application is directed to a method for data storage on a server in a telecommunications network. Claim 2 recites, in part, setting up a personal main folder on the server for a first user and configuring the personal main folder to have a functional locker that provides, *inter alia*, "a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user."

It is respectfully submitted that de Jong does not teach, or suggest, a personal locker that contains references to files of a first user that are displayable only to that first user, as required by claim 2. In contrast, de Jong merely describes a system that includes content database 340 or content repository 2708 that contains digital content from a content producer 2710, and a download manager 2716 in communication with a contents right database 2722 to determine whether a user requesting access to the content is an authorized user. De Jong, ¶¶ 0170-175; Fig. 27. The user 2702 of de Jong stores no reference to file of the user, as required by claim 2. De Jong fails to disclose, or suggest, that the content storer is the only user to which a reference to the content is displayable, as required by claim 2.

It is respectfully submitted that Challener fails to disclose the features of independent claim 2 demonstrated above to be missing from de Jong. Accordingly, a combination of de Jong and Challener, to the extent proper, could not render independent claim 2, nor any of its dependent claims, obvious.

Nor do any of Perlman, or Winiger teach or suggest the features of claim 2 demonstrated above to be missing from de Jong and Challener. Accordingly, any combination of de Jong,

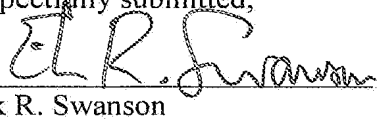
Challener, Perlman, and Winiger, to the extent proper, could not render independent claim 2, or dependent claims 3-16, obvious.

CONCLUSION

For all of the reasons set forth above, it is respectfully submitted that the rejections of claims 2-16 should be reversed. Appellants respectfully request that the rejections be withdrawn, and the case passed to allowance.

Dated: September 11, 2009

Respectfully submitted,

By 

Erik R. Swanson
Registration No.: 40,833
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(212) 527-7700
(212) 527-7701 (Fax)
Attorney For Applicant(s)

APPENDIXES

CLAIMS APPENDIX

The following is a copy of the claims involved in the appeal:

Claim 1 (Canceled)

Claim 2 (Previously presented): A method for data storage on a server in a telecommunications network, the telecommunications network providing connectivity between local computers of users and the server, the method comprising:

issuing, upon request, by an operator of the server, to a first user of the users a user certificate for access conditions;

providing the user certificate and a secret key to the first user;

accessing the server over an internet;

sending, by the server, a client program to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement;

setting up a personal main folder on the server for the first user, the main folder having a first special file including a first security requirement defined for the main folder and first management information so as to provide a main locker;

configuring the personal main folder to have at least one further folder set up therein, the at least one further folder having a function and a second file including a second security requirement defined for the least one further folder and including second management information so as to provide a functional locker;

displaying the functional locker only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, wherein the functional locker provides a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user, and at least one of:

a provisioning locker, wherein a first reference to a different second file available to another user is storable therein only by the first user; and

a receiving locker, wherein a third file of a second user of the users is storable therein only by the second user, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement.

Claim 3 (Previously presented): The method as recited in claim 2 wherein the certificate includes a public key.

Claim 4 (Previously presented): The method as recited in claim 2 further comprising providing a public key to the first user.

Claim 5 (Previously presented): The method as recited in claim 2 wherein the providing the user certificate and the secret key to the first user is performed by providing the user certificate and the secret key on a smart card.

Claim 6 (Previously presented): The method as recited in claim 2 wherein the at least one further security requirement includes at least one of a biometric system requirement, a geographic positioning requirement, a time restriction, a network requirement, and a computer data requirement.

Claim 7 (Previously presented): The method as recited in claim 6 wherein the at least one further security requirement includes a time dependency.

Claim 8 (Previously presented): The method as recited in claim 2 wherein the at least one further security requirement is a requirement of at least one of the operator of the server, the first user, and a sender of the third file.

Claim 9 (Previously presented): The method as recited in claim 2 wherein the provisioning locker has a name associated therewith.

Claim 10 (Previously presented): The method as recited in claim 2 wherein the provisioning locker includes a user locker for the another user.

Claim 11 (Previously presented): The method as recited in claim 2 wherein the receiving locker has a name associated with a sender of the third file.

Claim 12 (Previously presented): The method as recited in claim 2 wherein the receiving locker includes a user locker for the sender user.

Claim 13 (Previously presented): The method as recited in claim 2 wherein the first user and the second user are each registered with the server, and further including the steps of:

setting up a second personal main folder on the server for the second user, the second main folder having a respective first special file including a respective first security requirement defined for the respective main folder and respective management information so as to provide a respective locker,

configuring each respective main folder to have respective further folders set up therein, the respective further folders each having a respective function and each having a respective second file including a respective second security requirement defined for the respective further folders and including the respective management information, each of the further folders acting as a respective functional locker,

displaying each functional locker only if a respective security-relevant requirement is met, so as to provide a respective locker system having a virtual character, each functional locker providing a respective function of at least one of:

a respective personal locker, respective first files being storable in the respective personal locker only by the respective user and displayable only to the respective user;

a respective provisioning locker, wherein a respective first reference to a respective second file for a different user being storable by the respective user therein;

a respective receiving locker for a respective third file available to a respective sender user of the users, the respective receiving locker being configured, when opened, to provide to the respective user a respective sender user reference relating to the storage of the respective third file and to a respective sender user defined security requirement; and

a respective public locker configured to store, by the first user, the first reference to the second file when the first reference is stored in the provisioning locker, if access to the first reference is offered to a plurality of different users.

Claim 14 (Previously presented): The method as recited in claim 2 further including the steps of:

storing a fourth file in the functional locker only if the second security requirement is met;

generating a random number from data of the fourth file so as to provide an access key;

encrypting the data using the access key;

subsequently encrypting the access key with a public key and then destroying the access key so that the access key, for accessing the stored file, can only be recovered using the secret key;

receiving, at the server, the encrypted data, a fourth management information of the fourth file, and the encrypted access key;

encrypting, by the server, the transmitted encrypted data a second time;

generating a unique file identifier for the fourth file;

storing the fourth file in a system locker using the unique file identifier; and

storing a fourth reference to the fourth file in the functional locker, the fourth reference including the unique file identifier, the encrypted access key, and the fourth management information.

Claim 15 (Previously presented): The method as recited in claim 14 wherein the functional locker is the provisioning locker including a user file for the other user, and further including the steps of:

enabling the stored fourth file to be forwarded by the first user to the other user only if the first user decrypts the encrypted access key with the secret key and re-encrypts the decrypted access key with a second public key of the other user, and

storing the re-encrypted access key, the file unique identifier and the fourth management information, as the fourth reference to the file into the user locker.

Claim 16 (Previously presented): The method as recited in claim 14, wherein the second management information includes a management requirement, and wherein the storing the fourth file is performed only if the management requirement is met.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings for this matter.